6P

УДК 519.6

І.І. Рудик
Національний університет «Львівська політехніка»,
м. Львів, Україна
Україна, 79063, м. Львів, вул. Бандери, 12

Виявлення аномалій в комп'ютерній мережі на основі нейромережних технологій

I.I. Rudyk
National University "Lviv Polytechnic"
Ukraine, 79063, c. Lviv, Bandery str., 12

Model of Anomaly Detection in Computer Networks Based on Neural Network Technology

И.И. Рудик
Национальный университет «Львовская политехника»,
г. Львов, Украина
Украина, 79063, г. Львов, ул. Бандеры,12

Обнаружение аномалий в компьютерной сети на основании нейросетевых технологий

У статті проведено аналіз методів виявлення аномалій, які є частиною системи виявлення вторгнень. Проведено комп'ютерне моделювання нейромережного методу виявлення аномалій, який базується на аналізі поведінки користувачів. Основною перевагою розглянутих підходів є їх адаптивність, здатність до навчання та можливість виявлення не тільки відомих, але й нових видів атак.
Ключові слова: захист інформаційних систем, виявлення аномалій,
нейромережні технології, шаблон поведінки користувача.

With the rapid expansion of computer networks, security of using is getting actual. The paper analyses the methods for detection of anomalies that are a part of intrusion detection system. Computer simulation of neural network of anomaly detection system based on the analysis of user behavior. The main advantage of the considered system is its adaptability, learning ability and the ability to detect not only known but also new types of attacks.
Key Words: defence of the informative systems, exposure of anomalies,
neural network technologies, template of conduct of user.

В статье проведен анализ методов обнаружения аномалий, которые являются частью системы обнаружения вторжений. Проведено компьютерное моделирование нейросетевого метода обнаружения аномалий, который базируется на анализе поведения пользователей. Основным плюсом используемых подходов является их адаптируемость, стремление к обучению и возможность обнаружения не только известных, но и новых видов атак.
Ключевые слова: защита информационных систем, обнаружение аномалий,
нейросетевые технологии, шаблон поведения пользователя.

Вступ

Інформаційні технології все більше проникають у всі сфери людської діяльності. Інформація може представляти велику цінність та бути предметом купівлі-продажу.

Здебільшого саме через це інформаційні ресурси стають об'єктом атаки з метою їх заволодіння. Це призводить до того, що актуальним стає питання захисту. У зв'язку зі збільшенням обсягів інформації, що циркулюють в локальних обчислювальних мережах, та розширенням спектра завдань, що вирішуються за допомогою інформаційних систем, виникає проблема, пов'язана зі зростанням числа загроз і підвищенням вразливості інформаційних ресурсів [1].

Створення інформаційних систем, гарантовано стійких до шкідливих впливів і комп'ютерних атак, пов'язане з істотними витратами як часу, так і матеріальних ресурсів. Окрім того, існує відома зворотна залежність між зручністю користування системою та її захищеністю: чим досконаліші системи захисту, тим складніше користуватися основним функціоналом інформаційної системи. Ще у 80-і роки XX століття, в рамках оборонних проектів США, робилися спроби створення розподілених інформаційних систем спеціального призначення, які не повинні були виводитися з безпечного стану при будь-якій послідовності дій взаємодіючих об'єктів. У цих системах використовувалось спеціалізоване програмне забезпечення на всіх рівнях, включаючи системний. Але, на сьогоднішній день подібні системи не отримали розвитку, і для організації інформаційних систем використовуються операційні системи загального призначення, такі, як ОС Microsoft Windows, Linux та інші.

Огляд відомих підходів до побудови систем виявлення вторгнень

Створення ефективних підходів до захисту інформаційних систем зіштовхується також із браком обчислювальної потужності. З самого початку розвитку комп'ютерів і комп'ютерних мереж спостерігаються дві тенденції – щорічне подвоєння продуктивності обчислювачів, доступних за одну й ту ж вартість, та потроєння пропускної спроможності каналів зв'язку за той же період. Таким чином, зростання обчислювальної потужності вузлів мережі відстає від зростання обсягів переданої по мережі інформації, що з кожним роком посилює вимоги до обчислювальної складності алгоритмів систем захисту інформації [2].

Методи виявлення атак в сучасних системах недостатньо опрацьовані в частині формальної моделі атаки, і, отже, для них досить складно строго оцінити такі властивості, як обчислювальна складність, коректність, завершеність і т.д. Прийнято розділяти методи виявлення атак на методи виявлення аномалій і методи виявлення зловживань. Зловживання – це такий тип атак, у яких використовуються відомі недоліки інформаційних систем. Аномалія – це незвичайна активність в цілому, що може свідчити про вторгнення. Якщо зафіксована активність користувача відрізняється від очікуваної поведінки, то говорять про аномалію.

Більшість сучасних комерційних систем (Cisco IPS, ISS RealSecure, NFR) для протидії описаним вище загрозам використовують, здебільшого, сигнатурні (експертні) методи виявлення. Існує безліч академічних розробок у галузі виявлення аномалій, але в промислових системах вони використовуються рідко і з великою обережністю, оскільки такі системи породжують велику кількість помилкових спрацьовувань. Для експертних же систем основною проблемою є низька, близька до нуля, ефективність виявлення невідомих атак. Низька адаптивність до цих пір залишається проблемою, хоча такі переваги, як низька обчислювальна складність і мала вартість розгортання визначають домінування таких систем у даній сфері [3].

Постановка задачі

Зважаючи на сказане вище, **метою даної статті** є розробка такої моделі поведінки системи захисту, яка б дозволяла всі законні, хоч і нетипові дії користувача та блокувала незаконні. Складність побудови такої моделі полягає в тому, що неможливо створити всеосяжну систему виявлення, яка б передбачала всі можливі варіанти поведінки користувача. Для досягнення поставленої мети поступимо наступним чином. Змоделюємо не всі можливі варіанти, що є практично неможливим, а лише варіанти поведінки окремих користувачів. При такому підході окремо опишемо дозволені дії користувача стосовно інформаційної системи. Відслідкувати це в режимі реального часу теж непросто, оскільки дії користувача інформаційної системи далеко не завжди є однотипними та можуть варіюватися навіть в межах однієї сесії роботи. Описана ідея закладена в основу побудови детектора вторгнень, який зреалізований на основі нейронних мереж. При побудові нейронної мережі буде використано алгоритм зворотного поширення, який дасть можливість навчити систему ідентифікувати користувачів на основі команд, якими вони користуються при роботі. Для цього спочатку протягом деякого часу проводиться навчання запропонованого методу. Результатом такого навчання є формування гістограми команд для кожного користувача, яка в подальшому використовується як один з основних ідентифікаторів користувача.

Моделювання системи виявлення аномалій

До недавнього часу найбільш поширеною структурою системи виявлення вторгнень була модель, запропонована у роботі [1]. Її суть полягає в тому, що в більшості випадків побудова системи захисту мережі та антивірусних програм базувалася на використанні сигнатур – формальному описі відомих атак. Такі системи мали ряд недоліків. Найбільш суттєвими серед них є висока ймовірність помилкових спрацювань, низька швидкодія та відсутність механізмів виявлення нових атак. Це призвело до необхідності розробки нових підходів до створення систем виявлення вторгнень, які б характеризувалися вищим рівнем автоматизації та швидкодії і не вимагали великої кількості апаратних ресурсів. Припускається, що дії користувача та поведінка зловмисника відрізняються. Тому при побудові сучасних систем виявлення вторгнень використовують підхід, який базується на глибокому аналізі користувацької активності з метою її розпізнавання на нормальну та аномальну. Звичайно, такий підхід вимагає певного періоду часу на збір інформації про нормальну роботу системи та користувача, яка стає еталоном та відносно якої оцінюють всю решту дії. Також цей підхід має користуватися високим рівнем адаптивності стосовно кожного конкретного користувача.

Відомо декілька різновидів моделей систем виявлення аномалій. До найбільш поширених належать моделі, які базуються на прикладах поведінки користувача, частотні та нейромережні.

Один з найпростіших підходів до опису дій користувачів є підхід, який базується на описі поведінки користувачів. Пересічний користувач при роботі за комп'ютером працює в більшості випадків в одному середовищі, використовує певний обмежений набір програмних засобів та користується певним, але також обмеженим набором можливих команд k_i. З цього набору команд формується множина послідовностей команд $\{k_i\}$, які зазвичай виконує користувач. Такі ж множини послідовностей формуються під час навчання для всіх можливих користувачів та зберігаються у базі даних у вигляді профілів користувачів. При роботі користувача формується нова множина послідов-

ностей команд $\{k_i\}$, яка порівнюється кожним профілем у базі даних. Таким чином проводиться ідентифікація користувачів за їх діями. Суттєвий недолік такого підходу полягає у необхідності постійно зберігати профілі всіх користувачів та постійно моніторити послідовності дій користувача, що вимагає великої кількості програмних ресурсів.

Частотний підхід до опису дій користувача є подібним до попереднього. Різниця полягає в тому, що шаблони дій користувача представляються не у вигляді послідовностей команд, а у вигляді частоти їх появи та інших статистичних характеристик. Моніторингу підлягають вже не самі послідовності, а їх статистичні характеристики. Недоліком такого підходу є слабка адаптивність, а також те, що аналізується частота використання команд, а не їх послідовність.

При побудові системи виявлення аномалій у даній статті використано нейромережну модель. До основних переваг отриманої моделі можна віднести те, що навчивши систему на обмеженій кількості користувачів, вона узагальнює цю інформацію та формує очікувану реакцію у подібних ситуаціях. Паралельна обробка інформації у нейромережних системах дозволяє створювати достатньо швидкодіючі чи навіть он-лайн системи. В процесі навчання нейромережна система дає можливість виділяти ті найважливіші ознаки дій користувачів чи зловмисників, які формують базу для прийняття рішень. Ще однією важливою перевагою нейромережної моделі системи виявлення аномалій є можливість прогнозування роботи системи на основі її минулих дій.

Нейромережна система виявлення аномалій будується таким чином, що на її вхід подається набір параметрів, які характеризують роботу системи, а на виході отримуємо деякий коефіцієнт – здебільшого 1 чи 0, що характеризує наявність чи відсутність аномалій у її роботі. За вхідні параметри можуть бути використані час роботи користувача, які програми він використовує найбільше, швидкість набору команд і т.п. Такий підхід дає можливість не тільки виявляти аномалії, але й проводити ідентифікацію користувачів. Недоліком системи є те, що вона ефективно працює лише з невеликою кількістю користувачів, що є, здебільшого, цілком прийнятним для більшості комп'ютеризованих систем. При збільшенні кількості користувачів до тисяч ускладнюється ефективність їх розрізнення [4], [5].

Реалізація

Комп'ютерне моделювання проводилося в середовищі Matlab у додатку Neural Networks Toolbox.

При побудові моделі використовувалися багатошарові нейронні мережі прямого поширення. Їх навчання полягало в мінімізації функціонала помилки методом градієнтного спуску [5], під час якого по каналу від'ємного зворотного зв'язку здійснюється порівняння фактичних і заданих відповідей мережі.

Суть даної процедури полягає в пошуку величини зміни ваги зв'язку Δa_{ij} між i-м нейроном попереднього шару й j-м нейроном наступного. Розрахунок даної величини здійснюється послідовними наближеннями за циклічним алгоритмом методом градієнтного спуску, тобто величина Δa_{ij} визначається як частинна похідна за поточним значенням вагового коефіцієнта від середньоквадратичної функції помилки системи:

$$\Delta a_{ij} = -\alpha \frac{\partial M}{\partial a_{ij}},$$

де $M = 0{,}5\sum_j \left(y_j^{ф} - y_j^{з}\right)^2$ – функція помилки навчання, α – коефіцієнт інтенсивності навчання, a_{ij} – вага міжнейронного зв'язку, $y_j^{ф}$ – фактичний вихід j-го нейрона, $y_j^{з}$ – його заданий (необхідний) вихід.

Рішення даних рівнянь залежить від обраного типу граничної функції. Коефіцієнт α не повинен бути занадто великим, щоб забезпечувати стійкість навчання, і не занадто малим, щоб навчання надмірно не затягувати. Емпірично встановлений діапазон значень коефіцієнта швидкості навчання: $0 \div 1$, а рекомендується 0,1.

Застосування даного методу передбачає наявність впливу суб'єкта навчання, який повинен заздалегідь визначати вихідні відгуки об'єкта навчання для кожного вхідного впливу. Такий підхід навчання штучних нейронних мереж називається «навчанням із учителем». Але вихідні сигнали апріорі повинні перебувати в однозначному взаємозв'язку із вхідними сигналами.

Для побудови шаблону поведінки користувача було використано набір команд, який він використовує. Але такий підхід виявився неефективним для великої кількості користувачів. Тому надалі при побудові шаблону користувача використовувався не лише набір команд, але й враховувалася послідовність їх використання [1].

Далі, на основі кількості правильно передбачених команд робиться висновок про наявність чи відсутність аномалії у мережі. Якщо кількість вірно передбачених команд вища за певний експериментально встановлений рівень, то вважається, що поведінка користувача вважається нормальною, в іншому випадку – аномальною. При аномальній поведінці користувача потрібно проводити додатковий аналіз – або користувач різко змінив свою поведінку, чого не потрібно виключати, або – це дії зловмисника. З плином часу користувачі змінюють свою поведінку. Для врахування цього фактора час від часу систему потрібно додатково навчати, щоб вона адаптувалася до нових дій користувача.

Висновок

У даній статті розглянутий підхід до побудови системи виявлення вторгнень. Показано, що аналіз дій користувача є одним із ефективних засобів виявлення зловмисника у комп'ютеризованих системах. Як інструмент при реалізації даної системи використані штучні нейронні мережі. Це надало системі властивостей адаптивності та здатності до навчання при зміні поведінки користувача. В подальшому планується провести комп'ютерне моделювання розглянутого у роботі підходу у поєднанні з сигнатурними методами, що дозволить розробити високоефективну нейромережну систему виявлення вторгнень, яка виявлятиме не тільки відомі, але й нові види атак.

Література

1. Ryan J. Intrusion Detection with Neural Networks / Ryan J., Lin M.-J., Miikkulainen R. // Advances in Neural Information Processing Systems. – Cambridge, MA : MIT Press, 1998. – P. 254-272.
2. Большев А.К. Подход к обнаружению аномального трафика в компьтерных сетях с использованием методов кластерного анализа / А.К. Большев, В.В. Яновский // Известия Государственного Электротехнического Университета, серия Информатика, управление и компьютерные технологии. – 2006. – Выпуск 3/2006. – Изд-во СПбЭТУ, СПб. – С. 38-45.
3. Котенко И.В. Перспективные направления исследований в области компьютерной безопасности / И.В. Котенко, Р.М. Юсупов // Защита информации. Инсайд. 2006. – № 2. – С. 46-57.
4. Denning D. An Intrusion Detection Model / D. Denning // IEEE Transactions on Software Engineering. – 1987. – V. SE-13, № 1. – P. 222-232.
5. Головко В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпьютеры и их применение : [учеб. пособие]. – М., 2001. – 256 с.

Literatura

1. Ryan J. Advances in Neural Information Processing Systems. Cambridge. MA: MIT Press. 1998. P. 254-272.
2. Bol'shev A.K. Izvestija Gosudarstvennogo Jelektrotehnicheskogo Universiteta, serija Informatika, upravlenie i komp'juternye tehnologii. Vypusk 3/2006. Izd-vo SpbJeTU. SPb. 2006. S. 38-45.
3. Kotenko I. V. Zashhita informacii. Insajd. 2006. № 2. S. 46-57.
4. Denning D. IEEE Transactions on Software Engineering. V. SE-13. № I. 1987. P. 222-232.
5. Golovko V.A. Nejrokomp'jutery i ih primenenie: ucheb. posobie. M. 2001. 256 s.

I.I. Rudyk

Model of Anomaly Detection in Computer Networks Based on Neural Network Technology

In recent years, most of the information as private and proprietary stored as files in computer systems. Often this information is a trade secret. To prevent damage or theft of computer networks using a variety of software protection system. Most of these systems use signature detection methods. Their disadvantage is that they can only detect known attack signatures which is in the database system. Such systems are not adaptive and unable to detect new types of unknown threats. This has necessitated new approaches to the creation of protection systems that would allow counter not only known attacks but also to detect new types of them. The paper considers modern approaches to building information security systems. The idea of building such systems is based on that user's actions and behavior of different attacker. In this work the best known methods for identification of the user and attacker. These approaches are the basis of a detection system anomalies. Modeling user behavior pattern and found that it is one of effective means of identifying the attacker in computerized systems. When modeling used in multilayer networks, which provide an opportunity to study systems of protection and performance in the implementation.

Стаття надійшла до редакції 07.05.2012.